Yui Kee Computing Ltd.

Newsletter

April 2006

Contents

Incident Update

Tue Apr 18 15:46:12 2006 CA: Win32.Mydoom.N Medium

IE Exploit Fixed

Microsoft apparently decided that the Internet Explorer "createTextRange" vulnerability, reported in March and classified as “Critical” by Microsoft, did not warrant breaking its monthly security update schedule. The fix was released on 11 April 2006, almost three weeks after the vulnerability was revealed. In the intervening period, in-the-wild malware was actively exploiting the flaw.

However, the patch rollout was not without problems: it resulted in Windows Explorer issues for some users, prompting Microsoft to re-issue a corrected version on the 25th.

More information:

http://www.f-secure.com/weblog/archives/archive-042006.html#00000860

http://support.microsoft.com/kb/918165

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1359

http://www.f-secure.com/weblog/archives/archive-032006.html#00000842

Vista Security

At the same time some experts are saying that the “improved security” in Microsoft’s yet-to-be-released operating system, Windows Vista, will have little effect, other experts are claiming that one of the “security features”, “BitLocker Drive Encryption”, are anti-Linux.

Eugene Kaspersky, of Kaspersky Labs, and John Kay of Blackspider predicted the security measures would offer little protection. Kaspersky said, “Within a year there will be something like a rootkit for Vista" and Kay had a pessimistic view of code quality, expecting a "bug per line of code". Kay was also pessimistic about the outlook for ordinary users, "My wife and kids are going to continue to be subjected to all the threats out there [with the switch to Vista]. If you think about it, that's just crap."

Meanwhile, Bruce Schneier saw a dark side to technology touted to protect data from being revealed if a machine is lost or stolen, "You could look at BitLocker as anti-Linux because it frustrates dual boot." Schneier is also concerned that "endless" warning messages from Vista will lead many consumers to ignore them and blindly agree to what applications are seeking to do.

More information:

http://www.theregister.com/2006/04/27/schneier_infosec/

http://www.theregister.com/2006/04/27/av_on_ms/

Security Legal Minefield

Last June, San Diego-based information technology professional Eric McCarty discovered an SQL-injection flaw in the University of Southern California's online application system. He downloaded a small number of records to demonstrate the flaw existed and reported it to the University and SecurityFocus. The US Attorney's Office in the Central District of California has now charged McCaty with computer intrusion.

Michael Zweiback, an assistant US Attorney involved in the case said, "It wasn't that he could access the database and showed that it could be bypassed, he went beyond that and gained additional information regarding the personal records of the applicant. If you do that, you are going to face - like he does - prosecution."

There is a fine line for vulnerability researchers to tread between responsibly discovering flaws so that they can be fixed to prevent data theft crimes, and actually committing those crimes during the research.

More information:

http://www.theregister.com/2006/04/28/breach_suspect_prosecuted/

http://www.securityfocus.com/news/11341

http://www.securityfocus.com/brief/191

Dangerous sites uses Sudoku to lure users

The popular Sudoku puzzle is used as a bait by the hackers. They lure users to visit some dangerous websites, in the name of fully functional Sudoku puzzles. While the users are playing the Sudoku puzzles for fun, the vulnerable computers will automatically download adware without users' notices.

More Information:

http://www.theregister.co.uk/2006/04/10/yazzlesoduko/

Defeating Lazy Phishers

Mikko Hypponen, of F-Secure, suggests an easy way to catch out phishers who create their fake sites by linking to the real site's images.

More information:

http://www.f-secure.com/weblog/archives/archive-042006.html#00000856

Suite C & D, 8/F, Yally Industrial Building
6 Yip Fat Street, Wong Chuk Hang, Hong Kong
Tel: 2870 8550 Fax: 2870 8563
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/